EP 22665 (1)

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 768 534**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 11628**

(51) Int Cl$^6$ : **G 07 B 17/04**

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 18.09.97.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 19.03.99 Bulletin 99/11.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *NEOPOST INDUSTRIE SOCIETE ANONYME* — FR.

(72) **Inventeur(s)** : GILHAM DENNIS T.

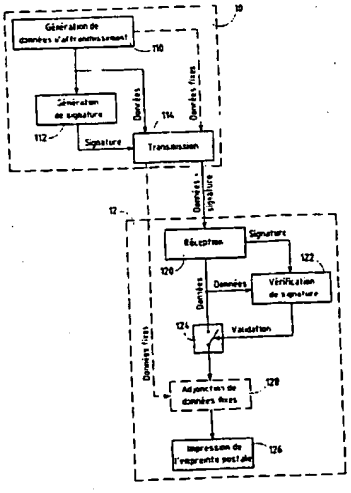
(73) **Titulaire(s)** :

(74) **Mandataire(s)** : CABINET BEAU DE LOMENIE.

## (54) PROCEDE ET DISPOSITIF DE SECURISATION DE DONNEES POSTALES.

(57) Procédé de sécurisation de données postales entre un dispositif de comptabilisation d'affranchissement (10) et un dispositif d'impression numérique à usage général (12), caractérisé en ce qu'il comporte les étapes suivantes:

- a) génération de données d'affranchissement dans le dispositif de comptabilisation,
- b) génération d'une signature numérique initiale à partir d'une partie déterminée de ces données d'affranchissement,
- c) transmission en clair des données d'affranchissement et transmission de la signature numérique initiale vers le dispositif d'impression numérique à usage général,
- d) réception des données d'affranchissement et de la signature numérique initiale,
- e) vérification de la signature numérique initiale reçue par élaboration d'une nouvelle signature numérique à partir de la partie déterminée des données d'affranchissement reçues et comparaison de cette nouvelle signature numérique avec la signature numérique initiale reçue, et
- f) impression de l'empreinte postale à partir des données d'affranchissement reçues en cas de résultat positif de ladite comparaison.




FR 2 768 534 - A1

Domaine de l'invention

La présente invention concerne le domaine du traitement de courrier et plus particulièrement celui des systèmes d'affranchissement modulaires mettant en œuvre des imprimantes numériques à usage général.

Art antérieur

Dans les systèmes modulaires d'affranchissement postal, les dispositifs de comptabilisation des affranchissements et d'impression des empreintes postales, qui étaient disposés avec les systèmes classiques (les machines à affranchir traditionnelles) dans une enceinte sécurisée et plombée pour interdire tout accès non autorisé, sont séparés l'un de l'autre et le dispositif d'impression est généralement simplement constitué d'une imprimante numérique à usage général, comme par exemple une imprimante laser ou bien à jet d'encre. La demande de brevet américain n° 562268 de la demanderesse aux noms de C.Shah et K.Robertson décrit un tel système d'affranchissement modulaire.

Toutefois, dans ce système où le dispositif d'impression est éloigné du dispositif de comptabilisation, il existe un risque très important de prélèvement des données échangées entre les deux dispositifs. Il peut en résulter une falsification des valeurs d'affranchissement avec comme conséquence un manque à gagner considérable pour l'administration postale.

Une solution à ce problème est donnée par le brevet US 5 583 779 qui propose un procédé pour sécuriser la liaison entre les dispositifs de comptabilisation et d'impression en rendant inintelligible les données échangées entre ces deux dispositifs au moyen d'algorithmes de chiffrement classiques, symétrique à clés secrètes tel que le DES (Data Encryption Standard) ou asymétrique tel que le RSA (Rivest-Shamir-Adelman) par exemple.

Ce procédé présente malheureusement deux inconvénients particulièrement importants qui en limite sa diffusion. Tout d'abord, certains de ces algorithmes qui font appel à des clés de chiffrement comportant un nombre de caractères très élevé sont considérés par certains Etats (par exemple les Etats Unis d'Amériques) comme des armes de guerre et en conséquence sont interdits à l'exportation. Ensuite, dans d'autres Etats (par exemple la France), ces algorithmes sont soumis à une autorisation

préalable du gouvernement, ce qui n'est pas sans poser quelques difficultés au niveau de la commercialisation des matériels les incorporant. Enfin, avec les algorithmes symétriques se pose le problème particulièrement complexe de la gestion (l'échange) des clés secrètes de chiffrement.

Définition et objet de l'invention

Aussi, la présente invention à pour objet un procédé qui permette un transfert d'informations entre le dispositif de comptabilisation d'affranchissement et le dispositif d'impression des empreintes postales qui soit imperméable aux interceptions non autorisées et pallie les inconvénients précités, c'est à dire notamment qui puisse être mis en oeuvre sans aucune autorisation de quelque type que ce soit et sans gestion complexe de clés de chiffrement.

Ce but est atteint par un procédé de sécurisation de données postales entre un dispositif de comptabilisation d'affranchissement et un dispositif d'impression numérique à usage général, caractérisé en ce qu'il comporte les étapes suivantes :

- dans le dispositif de comptabilisation
  - a) génération de données d'affranchissement,
  - b) génération d'une signature numérique initiale à partir d'une partie déterminée de ces données d'affranchissement,
  - c) transmission en clair des données d'affranchissement et transmission de la signature numérique initiale vers le dispositif d'impression,
- dans le dispositif d'impression numérique à usage général
  - d) réception des données d'affranchissement et de la signature numérique initiale,
  - e) vérification de la signature numérique initiale reçue par élaboration d'une nouvelle signature numérique à partir de la partie déterminée des données d'affranchissement reçues et comparaison de cette nouvelle signature numérique avec la signature numérique initiale reçue, et
  - f) impression de l'empreinte postale à partir des données d'affranchissement reçues en cas de résultat positif de ladite comparaison.

Avec ce procédé, il n'est plus nécessaire de chiffrer les données d'affranchissement qui peuvent maintenant être transmises en clair, la

validité de ces données étant garantie par la seule signature numérique qui les accompagne. Ce procédé qui ne fait pas appel à un échange de clés secrètes évite en outre les inconvénients de l'art antérieur liés à ce transfert entre le dispositif de comptabilisation d'affranchissement et le dispositif d'impression numérique.

Dans un mode de réalisation avantageux, l'étape de génération de signature comporte une étape préalable d'élaboration, à partir d'un protocole de hachage à sens unique appliqué à ladite partie déterminée des données d'affranchissement, d'un message réduit à partir duquel est élaborée ladite signature numérique initiale. L'étape de vérification de signature comporte alors une étape préalable d'élaboration, à partir dudit protocole de hachage à sens unique appliqué à ladite partie déterminée des données d'affranchissement reçues, d'un nouveau message réduit à partir duquel est élaborée ladite nouvelle signature numérique.

De préférence, la partie déterminée des données d'affranchissement comportent au moins les données alphanumériques suivantes : montant d'affranchissement, date de dépôt, numéro séquentiel de transaction.

Les données d'affranchissement délivrées par le moyen de génération comportent des données graphiques fixes qui sont transmises directement du dispositif de comptabilisation d'affranchissement au dispositif d'impression numérique pour être imprimés avec les autres données d'affranchissement sans procéder à l'élaboration d'une signature numérique de ces données fixes. Dans une variante de réalisation, ces données graphiques fixes peuvent être élaborées directement au niveau du dispositif d'impression numériques et sont imprimés avec les autres données d'affranchissement.

L'invention concerne également un système d'affranchissement pour la mise en oeuvre de ce procédé, lequel comporte au moins un dispositif d'impression numérique à usage général pour délivrer des enveloppes et/ou des étiquettes affranchies et un dispositif de comptabilisation d'affranchissement relié à distance de ce dispositif d'impression numérique. Ce dispositif d'impression numérique à usage général est constitué par une imprimante laser ou par une imprimante à jet d'encre.

Le système d'affranchissement peut comporter en outre une plieuse/ inséreuse pour plier et insérer des documents dans les enveloppes affranchies délivrées par le dispositif d'impression numérique à usage

général. Il peut également comporter une station de restauration de crédit reliée à distance au dispositif de comptabilisation d'affranchissement.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront mieux de la description suivante, faite à titre indicatif et non limitatif, en regard des dessins annexés, sur lesquels:

- la figure 1 montre de façon schématique les différents constituants d'un système d'affranchissement modulaire, et
- la figure 2 détaille les moyens de sécurisation des dispositifs de comptabilisation et d'impression du système de la figure 1.

Description détaillée d'un mode de réalisation préférentiel

La figure 1 illustre de façon très schématique un système d'affranchissement modulaire. Ce système est constitué de deux éléments principaux : un dispositif de comptabilisation d'affranchissement de sécurité (Secure Metering device SMD) 10 et un dispositif d'impression numérique 12. Bien entendu, une plieuse/inséreuse 14, une balance électronique 16 et une station de restauration de crédit 18 pourront compléter de manière connue ces deux éléments pour former un système complet de préparation de courrier.

Le SMD 10 réalise les fonctions de comptabilisation d'affranchissement généralement associées à une machine à affranchir traditionnelle. Il communique notamment au dispositif d'impression numérique les informations d'affranchissement nécessaires à une validation de la transaction et à une impression de l'empreinte postale. Ce dispositif d'impression 12 est avantageusement une imprimante numérique conventionnelle à usage général, par exemple une imprimante laser ou une imprimante à jet d'encre.

La communication de ces informations est toutefois susceptible d'être interceptée par des personnes non autorisées en vue de prélever et de falsifier le contenu de ces informations. Pour éviter cela, il est proposé selon l'invention non plus de chiffrer ces informations (c'est à dire d'assurer une fonction de confidentialité en les rendant inintelligibles) comme l'enseignait l'art antérieur mais seulement d'authentifier ces informations et de s'assurer de leur intégrité.

L'authentification de messages se distingue du chiffrement de messages en ce que contrairement à ce dernier il permet leur transmission en clair et surtout il ne nécessite pas d'autorisation spécifique et est donc totalement libre d'emploi.

La figure 2 montre un exemple préférentiel de réalisation de cette fonction d'authentification des données transitant entre le dispositif de comptabilisation d'affranchissement 10 et le dispositif d'impression numérique des empreintes postales 12.

Le dispositif de comptabilisation 10 comporte bien entendu un moyen de génération les informations ou données d'affranchissement 110. Par données d'affranchissement on entend classiquement les données alphanumériques comme le montant de l'affranchissement, les différentes valeurs des compteurs d'affranchissement (compteur ascendant et compteur descendant), la date de l'envoi, les numéros postaux du dispositif de comptabilisation et du client, le code de l'établissement postal de dépôt, le numéro séquentiel de transaction, éventuellement l'heure d'envoi, la catégorie de courrier, etc. et les données graphiques comme la partie fixe de l'empreinte postale (y compris l'estampille ou logo de l'administration postale ou une flamme publicitaire). Il peut être noté que l'adresse de destination peut avantageusement être considérée comme une donnée d'affranchissement.

Selon l'invention, le dispositif de comptabilisation comporte en outre un moyen de génération de signature 112 relié au moyen de génération des données d'affranchissement 110 et destiné à élaborer une signature numérique à partir de tout ou partie des données alphanumériques d'affranchissement. L'élaboration de la signature est effectuée au moyen d'algorithmes de signature connus en soi comme le DSA (Digital Signature Algorithm), les procédés de signature ElGamal ou Schnorr par exemple. Pour le calcul de ces algorithmes, ces techniques reposent sur l'utilisation d'une clé privée spécifique à un dispositif de comptabilisation d'affranchissement donné et d'une clé publique associée mais accessible à tous les dispositifs d'impression numérique. Avec ces techniques, le problème de l'échange des clés ne se pose plus puisque seul le dispositif de comptabilisation d'affranchissement dispose d'une clé secrète et que l'envoi des données s'effectue sans échange préalable d'information (notamment de clés).

Un moyen de transmission 114 relié à la fois au moyen de génération de données d'affranchissement 110 et au moyen de génération de signature 112 est prévu pour transmettre au dispositif d'impression 12 à la fois les données d'affranchissement et la signature numérique correspondante. Les données d'affranchissement sont transmises en clair (il s'agit des données graphiques et au moins une partie des données alphanumériques, comme le montant d'affranchissement ou la date de dépôt par exemple) et donc parfaitement lisibles par l'utilisateur, la signature numérique étant par contre un ensemble de caractères alphanumériques (par bloc de 64 bits en mode DSA par exemple) sans signification particulière.

Le dispositif d'impression numérique 12 comporte un moyen de réception 120 destiné à recevoir les informations (données d'affranchissement plus signature) transmises par le dispositif de comptabilisation d'affranchissement 10 et un moyen de vérification de signature 122 relié à ce moyen de réception pour valider les données d'affranchissement reçues. Ce moyen de vérification de signature comporte tout d'abord un moyen pour élaborer une nouvelle signature numérique à partir de ces données (en pratique à partir seulement d'une partie des données alphanumériques d'affranchissement ; bien entendu la même partie que celle ayant servie à l'élaboration de la signature initiale) par application du même algorithme de signature que celui ayant permis l'élaboration de la signature numérique initiale dans le dispositif de comptabilisation d'affranchissement 10 (mais cette fois au moyen de la clé publique). Il comporte ensuite un moyen pour comparer cette nouvelle signature à celle reçue par le moyen de réception 120 directement du dispositif de comptabilisation d'affranchissement et pour, en cas d'identité, générer un signal de validation pour un moyen de commutation 124 relié au moyen de réception 120 et assurant un aiguillage des données d'affranchissement reçues vers des moyens d'impression de l'empreinte postale 126.

La mise en œuvre du procédé selon l'invention est dès lors particulièrement simple. L'algorithme de signature est utilisé avec la clé privée du dispositif de comptabilisation pour signer des données d'affranchissement déterminées. De préférence, on adopte au moins les données suivantes : montant d'affranchissement, date de dépôt, numéro séquentiel de transaction. Le résultat de cette signature est envoyé au dispositif d'impression avec les données elles-mêmes. Le dispositif

d'impression utilise à son tour l'algorithme de signature avec cette fois la clé publique associée pour vérifier la signature et valider les données reçues. Ce procédé est bien meilleur que le seul chiffrement des données. En effet, la signature est infalsifiable car la clé privée est spécifique à un dispositif de comptabilisation d'affranchissement donné. Ensuite, la signature est authentique car la vérification par le dispositif d'impression est effectuée par la clé publique associée à la clé privée de l'expéditeur et toute falsification ne peut qu'aboutir à une absence de reconnaissance de la signature. Enfin, la signature n'est pas réutilisable car elle est fonction des données envoyées qui sont distinctes pour chaque article de courrier (datation, numéro séquentiel).

Une variante de ce mode de réalisation préférentiel est illustrée au niveau de cette figure 2 par des traits en pointillés. Dans cette variante, les données fixes de l'empreinte postale (par exemple le symbole graphique représentant l'estampille de l'administration postale : un aigle pour la poste américaine) qui ne servent pas à l'élaboration de la signature sont adressées directement au moyen de transmission 114 du dispositif de comptabilisation d'affranchissement 10 qui les délivrent au moyen de réception 120 du dispositif d'impression numérique 12 pour être intégrées au niveau d'un moyen d'adjonction 128 (disposé entre le moyen de commutation 124 et le moyen d'impression 126) aux autres données d'affranchissement validées par le moyen de vérification de signature 122. Dans une autre variante, ces données fixes sont élaborées directement dans le dispositif d'impression numérique 12.

Bien entendu, la présente invention ne se limite pas au seul mode préférentiel de réalisation décrit et des autres variantes ou compléments peuvent être envisagés sans sortir du cadre de l'invention. Notamment, avec le procédé de signature DSA, on peut constater que la longueur de la signature numérique est deux fois plus importante que celle des données à signer. Une solution à ce problème consiste à élaborer préalablement à la signature numérique, à partir d'un protocole de hachage à sens unique, par exemple issu du Secure hash standard (SHS) connu en soi, un message réduit (avantageusement sur 160 bits) qui servira de données de base pour l'élaboration de la signature telle que décrit précédemment. A la réception, ce message réduit est déterminé à nouveau à partir du même protocole appliqué cette fois aux données d'affranchissement reçues et une nouvelle

signature est alors élaborée à partir du message réduit obtenu. Le processus de vérification de la signature est ensuite poursuivi comme précédemment. De même, il peut être prévu au niveau du dispositif de comptabilisation d'affranchissement 10 des moyens de génération de code barres pour transmettre la signature sous la forme d'un code à barres, des moyens de réception de code barres étant alors prévus au niveau du dispositif d'impression numérique 12.

# REVENDICATIONS

1. Procédé de sécurisation de données postales entre un dispositif de comptabilisation d'affranchissement (10) et un dispositif d'impression numérique à usage général (12), caractérisé en ce qu'il comporte les étapes suivantes :

- dans le dispositif de comptabilisation

- a) génération de données d'affranchissement,

- b) génération d'une signature numérique initiale à partir d'une partie déterminée de ces données d'affranchissement,

- c) transmission en clair des données d'affranchissement et transmission de la signature numérique initiale vers le dispositif d'impression,

- dans le dispositif d'impression numérique à usage général

- d) réception des données d'affranchissement et de la signature numérique initiale,

- e) vérification de la signature numérique initiale reçue par élaboration d'une nouvelle signature numérique à partir de la partie déterminée des données d'affranchissement reçues et comparaison de cette nouvelle signature numérique avec la signature numérique initiale reçue, et

- f) impression de l'empreinte postale à partir des données d'affranchissement reçues en cas de résultat positif de ladite comparaison.

2. Procédé selon la revendication 1, caractérisé en ce que l'étape de génération de signature comporte une étape préalable d'élaboration, à partir d'un protocole de hachage à sens unique appliqué à ladite partie déterminée des données d'affranchissement, d'un message réduit à partir duquel est élaborée ladite signature numérique initiale.

3. Procédé selon la revendication 2, caractérisé en ce que l'étape de vérification de signature comporte une étape préalable d'élaboration, à partir dudit protocole de hachage à sens unique appliqué à ladite partie déterminée des données d'affranchissement reçues, d'un nouveau message réduit à partir duquel est élaborée ladite nouvelle signature numérique.

4. Procédé selon la revendication 1, caractérisé en ce que ladite partie déterminée des données d'affranchissement comportent au moins les

données alphanumériques suivantes : montant d'affranchissement, date de dépôt, numéro séquentiel de transaction.

5. Procédé selon la revendication 1, caractérisé en ce que lesdites données d'affranchissement délivrées par le moyen de génération (110) comportent des données graphiques fixes qui sont transmises directement du dispositif de comptabilisation d'affranchissement (10) au dispositif d'impression numérique (12) pour être imprimés avec les autres données d'affranchissement sans procéder à l'élaboration d'une signature numérique de ces données fixes.

6. Procédé selon la revendication 1, caractérisé en ce que lesdites données d'affranchissement comportent des données graphiques fixes qui sont élaborées directement au niveau du dispositif d'impression numérique (12) et sont imprimés avec les autres données d'affranchissement.

7. Système modulaire d'affranchissement postal mettant en œuvre le procédé selon l'une quelconque des revendications 1 à 6 comportant au moins un dispositif d'impression numérique à usage général (12) pour délivrer des enveloppes et/ou des étiquettes affranchies et un dispositif de comptabilisation d'affranchissement (10) relié à distance de ce dispositif d'impression numérique (12).

8. Système selon la revendication 7, caractérisé en ce que ledit dispositif d'impression numérique à usage général est constitué par une imprimante laser ou par une imprimante à jet d'encre.

9. Système selon la revendication 7, caractérisé en ce qu'il comporte en outre une plieuse/ inséreuse (14) pour plier et insérer des documents dans les enveloppes affranchies délivrées par le dispositif d'impression numérique à usage général (12).

10. Système selon la revendication 7, caractérisé en ce qu'il comporte en outre une station de restauration de crédit (18) reliée à distance au dispositif de comptabilisation d'affranchissement (10).

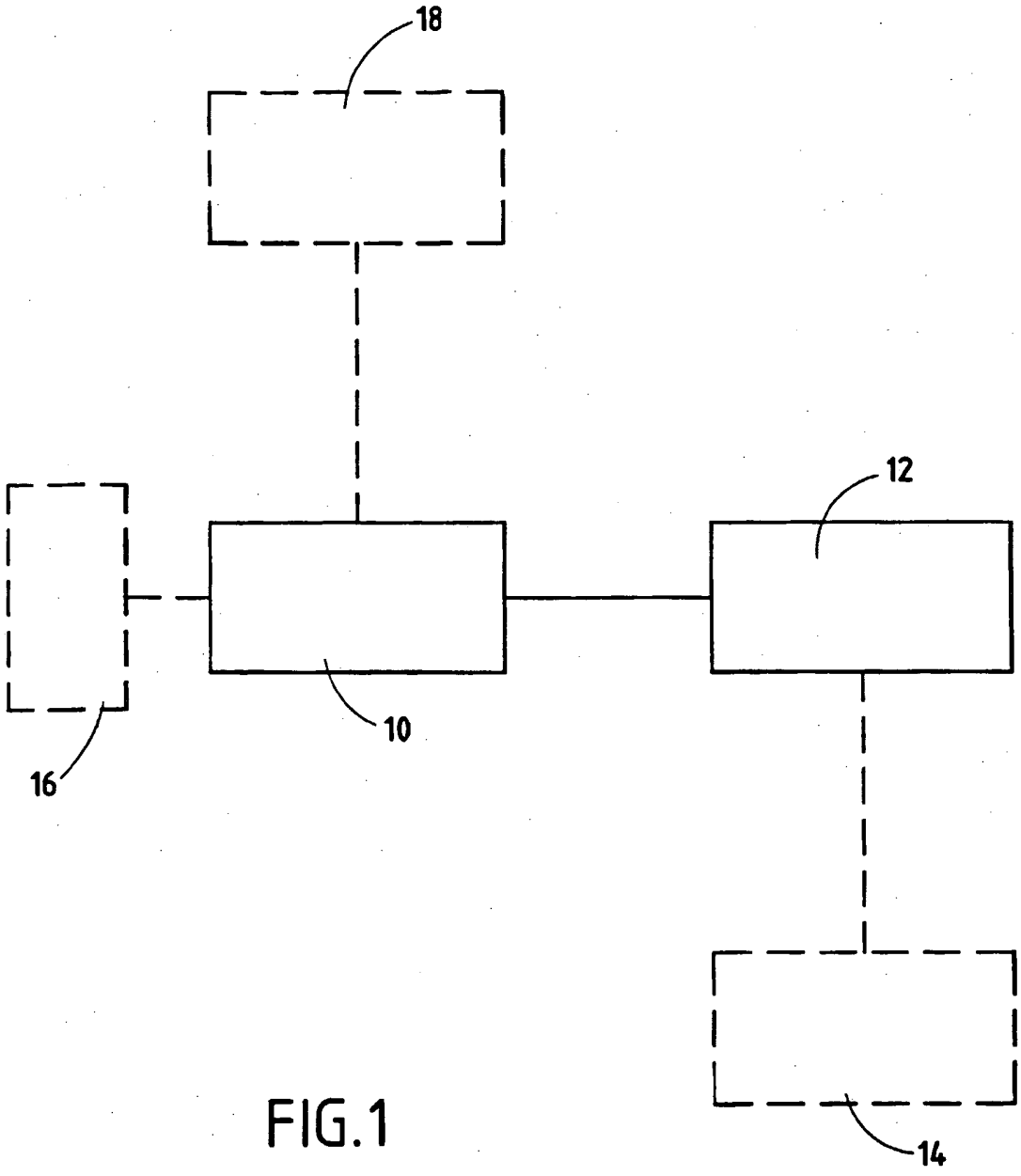



FIG.1

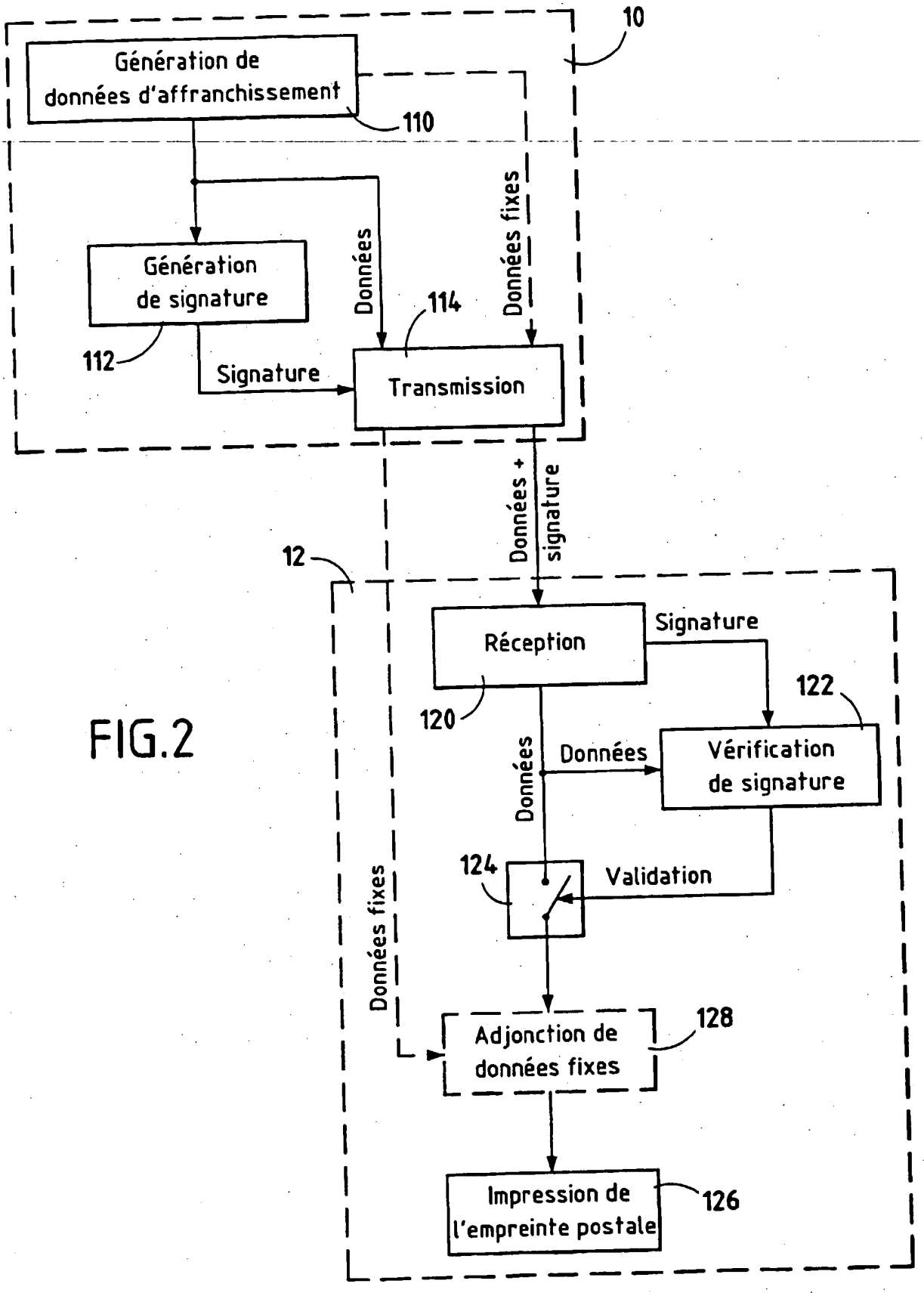

10
Génération de données d'affranchissement
110
Génération de signature
112
Signature
Données
Données fixes
114
Transmission
Données + signature
12
Réception
120
Signature
122
Vérification de signature
Données
Données
124
Validation
Données fixes
Adjonction de données fixes
128
Impression de l'empreinte postale
126

FIG.2

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

# RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2768534

N° d'enregistrement national

FA 548622
FR 9711628

| DOCUMENTS CONSIDERES COMME PERTINENTS | | Revendications concernées de la demande examinée |
|---|---|---|
| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | |
| A | EP 0 735 720 A (PITNEY BOWES) 2 octobre 1996<br>* revendication 1; figure 1 *<br>--- | 1-10 |
| A,D | US 5 583 779 A (NACLERIO EDWARD J ET AL) 10 décembre 1996<br>* revendication 1; figure 2 *<br>--- | 1-10 |
| A | EP 0 647 924 A (PITNEY BOWES) 12 avril 1995<br>* revendication 1; figure 1 *<br>--- | 1-10 |
| A | US 4 264 782 A (KONHEIM ALAN G) 28 avril 1981<br>* revendication 1; figure 1 *<br>--- | 1-10 |
| A | US 5 214 702 A (FISCHER ADDISON M) 25 mai 1993<br>* revendication 1; figure 2 *<br>--- | 1-10 |
| A | EP 0 741 375 A (PITNEY BOWES) 6 novembre 1996<br>* revendication 1; figure 1 *<br>----- | 1-10 |

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07B

| Date d'achèvement de la recherche | Examinateur |
|---|---|
| 12 juin 1998 | Kirsten, K |

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons



FORM 1503 03.82 (P04C13)